

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2003-516000

(P2003-516000A)

(43) 公表日 平成15年5月7日(2003.5.7)

(51) Int.Cl. ⁷	識別記号	F I	ターミナル [*] (参考)
H 0 4 Q 7/38		H 0 4 L 12/28	3 1 0 5 K 0 3 3
H 0 4 L 12/28	3 1 0	H 0 4 B 7/26	1 0 9 R 5 K 0 6 7
H 0 4 Q 7/22			1 0 7

審査請求 未請求 予備審査請求 有 (全 48 頁)

(21) 出願番号 特願2001-540557(P2001-540557)
 (86) (22) 出願日 平成12年11月21日(2000.11.21)
 (85) 翻訳文提出日 平成14年5月23日(2002.5.23)
 (86) 国際出願番号 P C T / I B 0 0 / 0 1 7 1 3
 (87) 国際公開番号 W O 0 1 / 0 3 9 5 3 8
 (87) 国際公開日 平成13年5月31日(2001.5.31)
 (31) 優先権主張番号 0 9 / 4 4 7 , 7 6 1
 (32) 優先日 平成11年11月23日(1999.11.23)
 (33) 優先権主張国 米国 (U S)

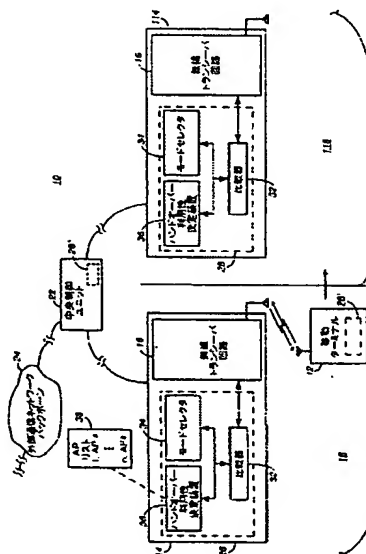
(71) 出願人 ノキア コーポレイション
 フィンランド エフイーエン-02150 エ
 スプー ケイララーデンティエ 4
 (72) 発明者 アラーラウリラ ユハ
 フィンランド エフイーエン-33210 タ
 ンペレ ムスタンラーデンカトゥ 10ア-
 5
 (72) 発明者 ハンセン ハリ
 フィンランド エフイーエン-02200 エ
 スプー ノキトンテュンクヤ 1エ-34
 (74) 代理人 弁理士 中村 稔 (外9名)

最終頁に続く

(54) 【発明の名称】 移動ターミナルハンドオーバー中のセキュリティ関連性の転送

(57) 【要約】

IEEE 802.11又はHIPERLANのような無線通信システムにおいて通信ハンドオーバー事象が発生したときに既存のセキュリティ関連性が再確立され、ワイヤレス通信ネットワーク内で通信ハンドオーバーが生じたときに移動ターミナルとそのネットワークとの間の既存のセキュリティ関連性が維持される。ハンドオーバー事象中の認証は、チャレンジ/応答手順によって達成される。このチャレンジ/応答手順によれば、新たなアクセスポイントと、この新たなアクセスポイントへのハンドオーバーを経験する移動ターミナルとで形成された通信対の各メンバーは、その通信対の他のメンバーへチャレンジを送信する。通信対の各メンバーは、次いで、その受信したチャレンジに対する応答を計算し、これら応答は、通信対の他のメンバーへ返送される。通信対の各メンバーは、次いで、その受信した応答を正しい応答と比較する。これら比較が正しいときには、第2アクセスポイントと移動ターミナルとの間でペイロード通信が開始される。



【特許請求の範囲】

【請求項1】 所定の移動ターミナルとの通信が第1アクセスポイントから第2アクセスポイントへハンドオーバーされるときに情報セキュリティを与える方法において、

複数のアクセスポイントを有する通信システムを用意し、各アクセスポイントは、上記通信システムによりサービスされる全地理的エリア内の異なる地理的エリアにサービスし、

上記全地理的エリア内で上記異なる地理的エリア間を各々物理的に移動可能な複数の移動ターミナルを用意し、

上記所定の移動ターミナルが上記第1アクセスポイントとの通信作用から上記第2アクセスポイントとの通信作用へ移動するときを感知し、

上記感知段階に応答して、上記第1アクセスポイントからセキュリティ関連性パラメータを検索し、その検索されたセキュリティ関連性パラメータに基づいて上記第2アクセスポイントにセキュリティ関連性を形成し、そしてその検索されたセキュリティ関連性パラメータに基づいて上記所定の移動ターミナルにセキュリティ関連性を形成し、そして

上記第1比較段階及び上記第2比較段階に基づいて上記所定の移動ターミナルと上記第2アクセスポイントとの間に通信を開始する、
という段階を備えた方法。

【請求項2】 上記の感知段階に応答して、上記所定の移動ターミナルから上記第2アクセスポイントへ認証アクセスポイントチャレンジを送信し、そして上記第2アクセスポイントから上記所定の移動ターミナルへ認証移動ターミナルチャレンジを送信し、

上記所定の移動ターミナルから受け取った上記認証アクセスポイントチャレンジに応答して上記第2アクセスポイントに認証アクセスポイント応答を発生し、

上記認証アクセスポイント応答を上記所定の移動ターミナルへ送信し、

上記第2アクセスポイントから受け取った上記認証移動ターミナルチャレンジに応答して上記所定の移動ターミナルに認証移動ターミナル応答を発生し、

上記認証移動ターミナル応答を上記第2アクセスポイントへ送信し、

上記認証アクセスポイント応答を上記所定の移動ターミナルにおいて正しい応答と第1比較し、

上記認証移動ターミナル応答を上記第2アクセスポイントにおいて正しい応答と第2比較し、そして

上記第1比較段階及び上記第2比較段階に基づいて上記所定の移動ターミナルと上記第2アクセスポイントとの間に通信を開始する、
段階を更に備えた請求項1に記載の方法。

【請求項3】 上記複数の移動ターミナルは、媒体アクセス制御層及び互換性物理層を有し、そして上記メッセージは、媒体アクセス制御メッセージである請求項2に記載の方法。

【請求項4】 上記メッセージは、IEEE802.11のようなワイヤレスLAN内に送信されるか、又はHIPERLAN/2マルチアクセスメッセージである請求項3に記載の方法。

【請求項5】 上記通信システムは、セキュリティプロトコルを使用してデータパケットの端一端セキュリティを与えるWLAN通信システムである請求項2に記載の方法。

【請求項6】 上記端一端セキュリティは、上記データパケットを認証及び／又は暗号化することにより与えられ、そして上記セキュリティプロトコルは、通信リンクの両端で同じ暗号及び／又は認証キーの使用を必要とする対称的暗号を与える請求項5に記載の方法。

【請求項7】 シール可能なキー管理プロトコルは、上記セキュリティプロトコルに対する対称的キーを発生するように動作する請求項6に記載の方法。

【請求項8】 上記所定の移動ターミナルと上記第2のアクセスポイントとの間にセッション従属動的暗号化キーを与え、そして

上記通信システムにより与えられる通信カバレッジ内で上記所定の移動ターミナルが移動するときに第1アクセスポイントから第2アクセスポイントへアクティブなセキュリティ関連性を転送する、
という段階を備えた請求項6に記載の方法。

【請求項9】 上記通信システムをLANとして用意し、

上記LAN内にサーバーを用意し、
通信ハンドオーバー中に通信が続くときに、端一端セキュリティ関連性に変更を必要とせずに、通信ハンドオーバー中に上記LAN内にキー管理及びセキュリティ関連性再確立を与え、上記通信ハンドオーバーが上記移動ターミナルと上記第1及び第2アクセスポイントとの間のセキュリティ機能にしか影響しないようにする、
という段階を備えた請求項4に記載の方法。

【請求項10】 上記LANは、上記複数のアクセスポイントと上記複数の移動ターミナルとの間にインターネットプロトコルセキュリティベースのセキュリティ関連性を含む請求項9に記載の方法。

【請求項11】 上記所定の移動ターミナル及び上記第1及び第2のアクセスポイントで作られた通信対の両端に対して認証キーが与えられ、この認証キーは、スケーリング可能なキー管理プロトコルにより発生される請求項1に記載の方法。

【請求項12】 上記所定の移動ターミナルと上記第1アクセスポイントとの間にはスケーリング可能なキー管理プロトコルに基づいて認証キー又はセキュリティ関連性が存在し、そして通信ハンドオーバー中に新たなキー交換の必要性を回避するために上記複数のアクセスポイント間にセキュリティ関連性が転送される請求項1に記載の方法。

【請求項13】 上記シール可能なキー管理プロトコルは、IKEであり、そして上記第1アクセスポイントから上記第2アクセスポイントへの上記通信ハンドオーバー中に新たなキー交換の必要性を回避するやり方で上記第1アクセスポイントと上記第2アクセスポイントとの間にセキュリティ関連性が転送される請求項12に記載の方法。

【請求項14】 キーを搬送するメッセージを暗号化する段階を含む請求項13に記載の方法。

【請求項15】 無線通信システムに通信ハンドオーバー事象が生じるときにセキュリティ関連性を維持するためのチャレンジ／応答方法において、
アクセスポイントと、このアクセスポイントへの通信ハンドオーバーを経験す

る移動ターミナルとで作られた通信対を用意し、

上記移動ターミナルから上記アクセスポイントへ第1チャレンジを送信し、

上記アクセスポイントから上記移動ターミナルへ第2チャレンジを送信し、

上記アクセスポイントにおいて上記受信した第1チャレンジに対する第1応答を計算し、

上記移動ターミナルへ上記第1応答を送信し、

上記移動ターミナルにおいて上記受信した第2チャレンジに対する第2応答を計算し、

上記アクセスポイントへ上記第2応答を送信し、

上記受信された第1応答を上記移動ターミナルにおいて正しい応答と第1比較し、

上記受信された第2応答を上記アクセスポイントにおいて正しい応答と第2比較し、そして

上記第1比較段階及び第2比較段階に基づき上記アクセスポイントと上記移動ターミナルとの間で通信を開始する、
という段階を備えた方法。

【請求項16】 上記無線通信システムは、グループIEEE802.11及びHIPERLANから選択される請求項15に記載の方法。

【請求項17】 上記移動ターミナルは、上記通信ハンドオーバー事象の前に別のアクセスポイントと通信状態にあり、そして上記セキュリティ関連性は、上記移動ターミナルと上記別のアクセスポイントとの間に存在するセキュリティ関連性である請求項15に記載の方法。

【請求項18】 第1通信アクセスポイントによりサービスされる第1地理的エリアから、第2通信アクセスポイントによりサービスされる第2地理的エリアへ移動ターミナルが物理的に移動するときに通信ハンドオーバーが発生するとき無線通信システムに所定のセキュリティ関連性を維持するための装置であって、上記移動ターミナルは、最初に、上記第1通信アクセスポイントと第1通信対を形成し、そして上記通信ハンドオーバーの後に、上記移動ターミナルは、上記第2通信アクセスポイントと第2通信対を形成し、上記第1通信対の各メンバー

は、それに関連した上記所定のセキュリティ関連性を有し、上記装置は、

上記移動ターミナルにあって上記通信ハンドオーバーを開始する必要性を感知するための第1手段と、

上記無線通信システム内にあって、上記第1手段が上記通信ハンドオーバーを開始する上記必要性を感知するのに応答して、上記第2通信アクセスポイントに上記所定のセキュリティ関連性を確立するための第2手段と、

上記移動ターミナルにあって、上記所定のセキュリティ関連性の関数としてアクセスポイントチャレンジを発生し、そしてそのアクセスポイントチャレンジを上記第2通信アクセスポイントへ送信するための第3手段と、

上記第2通信アクセスポイントにあって、上記第2通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数として移動ターミナルチャレンジを発生し、そしてその移動ターミナルチャレンジを上記移動ターミナルへ送信するための第4手段と、

上記移動ターミナルにあって、上記移動ターミナルチャレンジに応答して、上記所定のセキュリティ関連性の関数として移動ターミナル応答を発生し、そしてその移動ターミナル応答を上記第2通信アクセスポイントへ送信するための第5手段と、

上記第2通信アクセスポイントにあって、上記アクセスポイントチャレンジに応答して、上記第2通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数としてアクセスポイント応答を発生し、そしてそのアクセスポイント応答を上記移動ターミナルへ送信するための第6手段と、

上記移動ターミナルにあって、上記アクセスポイント応答に応答して、上記アクセスポイント応答が上記所定のセキュリティ関連性の関数として正しいかどうか決定するための第7手段と、

上記第2通信アクセスポイントにあって、上記移動ターミナル応答に応答して、上記移動ターミナル応答が、上記第2通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数として正しいかどうか決定するための第8手段と、

上記無線通信システムにあって、上記第8及び第9手段に応答して、上記移動

ターミナル応答及び上記アクセスポイント応答の両方が正しいときに上記通信ハンドオーバーを確立するための第9手段と、
を備えた装置。

【請求項19】 上記無線通信システムは、グループIEEE802.11及びHIPERLANから選択される請求項18に記載の装置。

【請求項20】 移動ターミナルの通信ハンドオーバーが発生するとき無線通信システムに所定のセキュリティ関連性を維持するための方法であって、上記移動ターミナルは、最初に、第1通信アクセスポイントと第1通信対を形成し、そして上記通信ハンドオーバーの後に、上記移動ターミナルは、第2通信アクセスポイントと第2通信対を形成し、上記第1通信対の各メンバーは、それに関連した上記所定のセキュリティ関連性を有し、上記方法は、

上記通信ハンドオーバーを開始する必要性を感知し、

上記通信ハンドオーバーを開始する上記必要性に応答し、そしてそれに応答して上記第2通信アクセスポイントに上記所定のセキュリティ関連性を確立し、

上記移動ターミナルに、上記所定のセキュリティ関連性の関数としてアクセスポイントチャレンジを発生し、

そのアクセスポイントチャレンジを上記第2通信アクセスポイントへ送信し、

上記第2通信アクセスポイントに、上記第2通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数として移動ターミナルチャレンジを発生し、

その移動ターミナルチャレンジを上記移動ターミナルへ送信し、

上記移動ターミナルにおいて上記移動ターミナルチャレンジに応答して、上記所定のセキュリティ関連性の関数として移動ターミナル応答を発生し、

その移動ターミナル応答を上記第2通信アクセスポイントへ送信し、

上記第2通信アクセスポイントにおいて上記アクセスポイントチャレンジに応答して、上記第2通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数としてアクセスポイント応答を発生し、

そのアクセスポイント応答を上記移動ターミナルへ送信し、

上記移動ターミナルにおいて上記アクセスポイント応答に応答して、上記アク

セスポイント応答が上記所定のセキュリティ関連性の関数として正しいかどうか決定し、

上記第2通信アクセスポイントにおいて上記移動ターミナル応答に応答して、上記移動ターミナル応答が、上記第2通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数として正しいかどうか決定し、そして

上記移動ターミナル応答及び上記アクセスポイント応答の両方が正しいときに上記通信ハンドオーバーを確立する、
という段階を備えた方法。

【発明の詳細な説明】**【0001】****【技術分野】**

本発明は、ワイヤレスローカルエリアネットワーク（WLAN）が非限定例である無線通信システムに係る。より詳細には、本発明は、移動ターミナルが第1ベースステーション又はアクセスポイント（AP）から第2ベースステーション又はアクセスポイント（AP）へハンドオーバーされるときに情報セキュリティを与えることに係る。

【0002】**【背景技術】**

最小限の構成においては、通信システムが送信ステーション及び受信ステーションで形成され、それらが通信チャンネルにより相互接続される。送信ステーションにより発生された通信信号は、通信チャンネルに送信され、そして受信ステーションにより受信される。

無線通信システムでは、通信チャンネルの少なくとも一部分が電磁スペクトルの一部分によって形成される。無線通信システムでは、送信ステーションと受信ステーションとの間に固定接続やハード布線接続が要求されないので、通信移動度を高めることができる。

【0003】

セルラー電話システムが一例であるセルラー通信システムは、無線通信システムの一例である。セルラー通信システムに対する加入者の移動ターミナルが、セルラー通信システムのネットワークインフラストラクチャーによって包囲されたエリア全体にわたりせいぜいどこかの位置に物理的に配置されるだけであるときには、移動ターミナルは、セルラー通信システムによって別の移動ターミナルと通信することができる。

例示的なワイヤレス通信システムのネットワークインフラストラクチャーは、各々トランシーバを含む物理的に離間されたベースステーション又はアクセスポイント（AP）を備えている。このような例示的システムでは、各ベースステーション又はAPは、通信システムの地理的エリア即ちセルを定義する。第1移動

ターミナルを使用して第2移動ターミナルと通信を行い、そして第1移動ターミナルがシステムのセル間を進行又は移動するときには、1つのベースステーションから別のベースステーションへのハンドオーバー通信により中断のない通信を行うことができる。このような通信ハンドオーバーは、ハンドオーバープロセスにより与えられる。

【0004】

HIPERLAN形式-2のような高性能の無線ローカルエリアネットワークは、3種類のハンドオーバーをサポートする。HIPERLAN/2は、ポータブル装置とブロードバンドIP、ATM及びUMTSネットワークとの間に高速（通常25Mb/sのデータレート）通信を与え、そして多数の媒体アプリケーションをサポートすることができ、典型的なアプリケーションは屋内である。HIPERLAN/2は、IP、ATM又はUMTSバックボーンに通常接続されたアクセスポイントと対話する移動及び固定ターミナルにより異なるインフラストラクチャーネットワーク（例えば、IP、ATM及びUMTS）へのローカルワイヤレスアクセスを与える。ネットワークにサービスするために多数のアクセスポイントが必要とされる。ワイヤレスネットワークは、全体として、移動性を与えるためにアクセスポイント間の接続のハンドオーバーをサポートする。典型的な動作環境は、ビジネスネットワーク及び家庭設備ネットワークを含む。HIPERLAN/2アクセスネットワークの概要は、参考としてここに取り上げるヨーロッパ・テレコミュニケーションズ・スタンダーズ・インスティテュート（ETSI）ドキュメントDTR/BRAN-00230002、1998年に掲載されている。

【0005】

移動ターミナルのハンドオーバー判断に基づいて、セクターハンドオーバー（インターセクター）、無線ハンドオーバー（インターアクセスポイントトランシーバ/インターアクセスポイントハンドオーバー）、ネットワークハンドオーバー（インターアクセスポイント/インターネットワークハンドオーバー）、又は強制ハンドオーバーがHIPERLAN/2に従って生じる。

ハンドオーバーを実行する前に、移動ターミナルは、現在アクセスポイントに

より使用される周波数、及びハンドオーバーに対する候補であるアクセスポイントにより使用される周波数に関する当該測定値を収集しなければならない。サービング周波数の測定は、移動ターミナルが現在アクセスポイントに同期される間に移動ターミナルにより実行することができる。しかしながら、隣接するアクセスポイントの周波数を測定するためには、移動ターミナルが現在アクセスポイントから一時的に不存在にならねばならない。

【0006】

移動ターミナル不存在手順の間に、移動ターミナルは、現在アクセスポイントから一時的に切断され、移動ターミナルは、隣接アクセスポイントに対する測定を行うことができる。この時間中には、移動ターミナルと現在アクセスポイントとの間で通信を行うことはできない。この不存在手順の一部分として、移動ターミナルは、それが n フレームの間不存在になることを現在アクセスポイントに告げる。この不存在周期の間に、移動ターミナルは、現在アクセスポイントにより到達することができない。この不存在周期の後、現在アクセスポイントは、移動ターミナル活性化シーケンスをトリガーし、移動ターミナルを使用できるかどうかチェックする。

【0007】

セクターハンドオーバー中には、アクセスポイントのアンテナセクターが変更され、同じアクセスポイントが全ハンドオーバーを制御する。セクターハンドオーバーが成功した後、移動ターミナルは、新たなセクターを経て通信する。無線ハンドオーバーは、アクセスポイント当たり2つ以上のトランシーバ、例えば、2つのアクセスポイントトランシーバと、1つのアクセスポイントコントローラとを有するアクセスポイントに関連している。無線ハンドオーバーは、移動ターミナルが、1つのアクセスポイントのカバレッジエリアから、同じアクセスポイントによりサービスされる別のカバレッジエリアへ移動するときに、実行される。無線ハンドオーバーは、データリンク制御(DLC)層内で実行できるので、上位層プロトコル(HL)は含まれない。移動ターミナルが、別のアクセスポイントコントローラへのハンドオーバーの必要性を検出したとき、移動ターミナルは、現在アクセスポイントに依然同期することができる。この場合に、移動ター

ミナルは、それが別のアクセスポイントコントローラへのハンドオーバーを遂行することをそのアクセスポイントコントローラに通知する。無線ハンドオーバーの場合は、進行中の接続、セキュリティパラメータ等に関する全ての当該情報がアクセスポイントに得られ、従って、この情報は再ネゴシエーションされない。

【0008】

ネットワークハンドオーバーは、移動ターミナルが1つのアクセスポイントから別のアクセスポイントへ移動するときに実行される。移動ターミナルは、無線制御リンク(RLC)インスタンスのサービスエリアを立ち去るので、ネットワークハンドオーバーは、収斂層(CL)及びHL(必要に応じて)並びにDLCIを含む。HL関連性及び接続を維持するために、バックボーンを通る特定のシグナリングが必要となる。移動ターミナルは、別の(ターゲット)アクセスポイントへのハンドオーバーの必要性を検出すると、現在アクセスポイントに依然同期されてもよい。この場合に、移動ターミナルは、それが別のアクセスポイントへのハンドオーバーを実行することを現在アクセスポイントに通知する。通知されたアクセスポイントは、次いで、その移動ターミナルへの通信を停止するが、指示があったときには特定の時間中その関連性を維持しなければならない。

【0009】

強制ハンドオーバーは、現在アクセスポイントのセルを立ち去るようある移動ターミナルに命令する機会を現在アクセスポイントに与える。強制ハンドオーバーは、アクセスポイントがForce_Handover信号を移動ターミナルに送信することにより開始される。1つの手順において、移動ターミナルは、新たなセルを見つけるかどうかに関わりなく、通常のハンドオーバーを実行してその古いセルを立ち去る。第2の手順では、移動ターミナルは、ハンドオーバーが失敗した場合に古いアクセスポイントに戻る機会を有する。

HIPERLAN/2特徴のこれ以上の説明については、参考としてここに取り上げるETSI規格化団体により提供された「ブロードバンド無線アクセスネットワーク(BRAN):HIPERLAN形式2機能的仕様:無線リンク制御(RLC)」を参照されたい。

【0010】

限定された地理的エリア、例えば、ビルやビル内のオフィス仕事場により包囲された限定されたエリアを包囲するために、多数の形式のワイヤレス通信システムが実施されそして他のものが提案されている。マイクロセルラーネットワーク、プライベートネットワーク及びWLANのようなワイヤレス通信システムは、このようなシステムの一例である。

ワイヤレス通信システムは、通常、取締り又は準取締り団体により施行された規格に準拠して構成される。例えば、IEEE（インスティテュート・オブ・エレクトリカル・アンド・エレクトロニック・エンジニアリング）により施行されたIEEE 802.11規格は、一般に商業用2.4GHzワイヤレスLANに関するワイヤレスローカルエリアネットワーク（LAN）規格である。この802.11規格は、ワイヤレスターミナルとベースステーションとの間及びワイヤレスターミナル間のインターフェイスを規定する。物理層及び媒体アクセス制御（MAC）層に関する標準は、このような規格に規定されている。この規格は、互換性のある物理層を含む種々の装置間に自動的に媒体を振り分けできるようにする。この規格においては、一般に、MAC層により、衝突回避（CSMA/CA）通信スキムを伴う搬送波感知多重アクセスを使用して、非同期データ転送が行われる。

【0011】

IEEE 802.11規格は、このような規格に準じて相互に動作できるように構成された移動ターミナルを使用することによりワイヤレス通信を行うためのものであるが、リアルタイムワイヤレスサービスについては十分に規定していない。例えば、この規格を実施する場合に、あるAPから別のAPへの通信ハンドオーバー中に著しいクオリティロスに時々遭遇する。相当数のデータフレームが失われるか又は遅延され、その結果、通信クオリティが失われるか、又は通信が終了することすらある。それ故、特にリアルタイムワイヤレスサービスについては、IEEE 802.11規格に規定された以外の動作モードが必要とされる。既存のIEEE 802.11規格に準じた動作に比して通信クオリティの改善を許す所有権付き機能が提案されている。このような所有権付き機能を実行するように動作できるAP及び移動ターミナルは、所有権モード可能と称される。

【0012】

しかしながら、移動ターミナルと、移動ターミナルが通信するときに通るAPとで構成された通信対の両端は、所有権モードでの動作が可能でなければならない。通信対の両端が所有権モードに準じて一緒に動作できない場合には、IEEE 802.11規格に準じた従来の動作が必要とされる。それ故、通信対の両端が所有権モードで動作するのを許す前に、通信対の両端が所有権モードに準じて動作できる能力について決定しなければならない。

上記の特許出願は、通信対の両端が所有権モードで一緒に動作できるかどうか識別するよう動作できる装置を提供する。この装置は、対の互換性が存在すると決定されたときに所有権モードで動作するように通信対の両端をアクチベートし、そしてその後、移動ターミナルが、第1APによりサービスされるセルから、第2APによりサービスされるセルへ物理的に移動したとすれば、ハンドオーバー手順の間に所有権モード動作を維持するように動作する。

【0013】

この特許出願の装置により与えられる貴重な特徴に加えて、このようなAP-APハンドオーバーが発生するときにセキュリティ関連性を再確立することが望ましい。

多くの顧客、特に、ビジネス環境は、高度なデータセキュリティを必要としており、このデータセキュリティは、WLANインストールを使用することにより妥協することができない。WLANへのアクセスは、物理的に制限することができないので、送信されたデータ及びネットワーク要素を保護するために、暗号化方法を使用することが習慣となっている。現在のIEEE 802.11及びITFインターネット規格は、ワイヤレスリンクを経ての機密データ通信即ちインターネットプロトコルセキュリティ(IPSEC)を与えるための2つの相補的なメカニズムを与える。このIPSECは、2つのIPホスト間にFOR機密通信を与えるIPベースのセキュリティプロトコルである。IPSECプロトコルは、バーチャルプライベートネットワーク(VPN)を構築する際に一般に使用される。

【0014】

WLANシステムでは、IPsecプロトコルを使用して、データパケットに対する端一端セキュリティを与えることができ、このセキュリティは、送信されるデータパケットを認証及び／又は暗号化することにより与えられる。IPsecは、対称的な暗号化を使用し、これは通信リンクの両端に同じ暗号及び／又は認証キーを使用する必要がある。IKEのようなシール可能なキーマネージメントプロトコルを使用して、IPsecスタックに対する対象的キーを発生することができる。

インターネットキー交換（IKE）のキーマネージメントプロトコルは、初期の移動ターミナル／アクセスポイント間連中にIPレベルセキュリティ関連性を確立するのに有用であるが、通信ハンドオーバーの必要が生じたときには、IKE又は他の同様のプロトコルの使用がハンドオーバーの実行に著しい時間遅延を与える。というのは、このようなプロトコルは、多数のメッセージの交換を必要とし、パブリック暗号キーの使用が多大な計算を必要とするからである。ペイロードトラフィックのハンドオーバーは、新たなAPと移動ターミナルとの間にアクティブなセキュリティ関連性が確立された後でなければ再開できないので、IKEキー管理プロトコル又は他のこのようなプロトコルを使用すると、ハンドオーバー中に問題が生じる。

【0015】

動的な暗号キー即ちセッション依存の動的なキーを伴うセキュリティプロトコルが移動ターミナルとAPとの間に適用されたときには、移動ターミナルが、ワイヤレス無線ネットワーク又はシステムにより形成されるカバレッジ内を移動するときに、あるAPから別のAPへアクティブなセキュリティ関連性を転送するためのメカニズムを見出すことが望ましい。

このような背景情報に鑑み、本発明は、WLAN通信ハンドオーバー中にキーを管理しそしてセキュリティ関連性を再確立するための低又は短遅延の方法／装置であって、ハンドオーバー中に端一端セキュリティ関連性（例えば、移動ターミナルとサーバーとの間のIPsecペイロード接続）を変更する必要がなく、そしてハンドオーバーが移動ターミナルと新たな及び古いAPとの間のセキュリティ機能にしか影響しないような方法／装置を提供する。

【0016】

【発明の開示】

本発明は、無線通信、IEEE802.11 2.4GHz WLAN規格、高性能無線ローカルエリアネットワーク（HIPERLAN）、ETSI HIPERLAN形式2規格、及びワイヤレスターミナルとネットワーク要素との間のIPSECレベルセキュリティ関連性に係る。本発明は、ETSI BRANやIEEE802.11を一例として含むいかなるIPベースのワイヤレスネットワークにも使用することができる。更に、本発明は、移動ターミナルが2つのIPSECルーターエンティティ間を移動するときに、ワイヤレスターミナルが、ワイヤレスアクセスポイントでないエンドポイントと通信する場合に使用することができる。

【0017】

本発明は、IEEE802.11又はHIPERLANのような無線通信システムにハンドオーバー事象が発生するときに既存のセキュリティ関連性を再確立するための効率的な方法／装置を提供する。本発明の動作は、ハンドオーバーの性能を高め、そして新たなAPと移動ターミナルとの間のセキュリティ関連性を再ネゴシエーションするのに関連した遅延を最小にする。

本発明は、ネットワーク内にハンドオーバーが発生するときに移動ターミナルとワイヤレス通信ネットワークとの間に確立されたセキュリティ関連性を維持する効率的な方法を提供する。本発明を利用する一例は、WLAN内の移動ターミナルとAPとの間にインターネットプロトコルセキュリティ（IPsec）ベースのセキュリティ関連性を有するWLANである。しかしながら、本発明は、HIPERLAN／2無線レベルセキュリティ機能のようないかなる形式の動的セキュリティ関連性を維持するのにも使用できる。

【0018】

本発明によれば、ハンドオーバー事象中の移動ターミナルの認証は、チャレンジ／応答手順により達成される。このチャレンジ／応答手順によれば、新たなAPが移動ターミナルにチャレンジを送信し、移動ターミナル（MT）は、それに応答して、新たなAPに応答を送信する。

移動ターミナルとAPとで作られる通信対の両端に対する認証キーは、最初に、スケーリング可能なキーマネジメントプロトコル、例えば、インターネットキー交換（IKE）により発生される。各ハンドオーバー中に新たな及び異なるキーの交換の必要性を回避するために、ワイヤレス通信システム内にある種々のAP間でセキュリティ関連性が転送される。

【0019】

キー及びそれに関連した情報は、ハンドオーバープロセス中に新たなAPにより要求され、そしてキー及び他の情報は、古いAPと新たなAPとの間を通過する1つ以上のハンドオーバーメッセージにおいて古いAPから新たなAPへ転送される。認証チャレンジの交換及びそれに対する応答は、新たなAPと、ハンドオーバーに含まれる移動ターミナルとの間に生じるハンドオーバーシグナリングに一体化される。

本発明の特徴によれば、メッセージは、媒体アクセス制御（MAC）メッセージである。

アクセスポイント認証を与える本発明の特徴は、望ましいものであるが、任意の特徴であることに注意されたい。

アクセスポイント間では機密の接続が好ましいが、このような特徴は、本発明の精神及び範囲によって要求されるものではない。

【0020】

【発明を実施するための最良の形態】

本発明のこれら及び他の特徴並びに効果は、添付図面を参照した以下の説明により当業者に明らかとなる。

図1は、移動ターミナル12が一例である複数の移動ターミナル間で及びそれらと無線通信するための通信システムを例示する図である。別の例では、アクセスポイントが無線インターフェイス及び固定ネットワークブリッジをカバーし、アクセスポイントが固定ネットワークに接続され、この例は、図1に示すCCUを必要としない。通信システム10は、IEEE802.11規格に規定されたように、そしておそらくは上記特許出願に開示された所有権付きの動作モードに準拠するように、複数の移動ターミナル12との無線通信を与えるWLANを形

成する。他の通信システムも同様であり、本発明の動作は、このような他の通信システムでも作用し得る。

【0021】

WLAN10は、2つの離間された地理的位置に個々に配置された複数の離間されたAP14及び114を含む。2つのAP14、114しか示されていないが、実際には、非常に多数のAPが使用される。AP14、114は、ベースステーション又はリモートアンテナ装置(RAD)とも称される。「アクセスポイント」、「AP」又は「ap」という語は、ここでは、通信システム10のネットワークインフラストラクチャーにアクセスするポイントを形成する装置を示すために一般的に使用される。「移動ターミナル」、「MT」又は「mt」という語は、アクセスポイントにアクセスするポイント形成する装置を示すために一般的に使用される。

【0022】

AP14、114の各々は、移動ターミナルが特定のAPの通信範囲内に位置するときに移動ターミナル12と無線通信信号をやり取りすることのできる無線トランシーバ回路16を備えている。一般に、移動ターミナル12は、所定のアクセスポイントの近くにあつて且つそれにより定義された地理的エリア即ちセル18、118内に位置するときに、AP14、114と通信する。図1において、セル18はアクセスポイント14に関連され、移動ターミナル12はセル18内にあり、そしてセル118は、アクセスポイント114に関連している。モードセクタ34は、本発明が所有権付き無線リンクレベルメッセージを使用して実施されるときだけ含まれ、これは、本発明に必須の実施ではない。

【0023】

アクセスポイント14、114は、中央制御ユニット(CCU)22に接続される。このCCU22は、通常、ハブ又はIPルーターである。CCU22は、外部通信ネットワークバックボーン24への接続を与える。図示されていないが、通常、他の通信ステーション及び他の通信ネットワークのような他の通信装置が通信ネットワークバックボーン24に接続される。このように、移動ターミナル12と、通信ネットワークバックボーン24に直接的又は間接的に接続された

通信ステーションとの間に通信を与えるように、通信経路を形成することができる。又、複数の移動ターミナル12間のローカル通信も許される。移動ターミナル12の対間の通信においては、それらの間に形成される通信経路が2つの個別の無線リンクを含む。

【0024】

AP14、114は、各APの動作に関連した種々の制御機能を実行する制御要素28を備えている。図1において、制御要素28は、各々、比較器32、モードセクタ34及びハンドオーバー利用性決定装置36を含むように示されており、これらの制御要素は、機能的なもので、例えば、処理回路により実行できるアルゴリズムのような所望のやり方で実施される。別の実施形態では、このような要素により実行される機能は、どこかに配置され、例えば、ブロック28'で示すように移動ターミナル12に配置されるか、又はブロック28''で示すようにCCU22に配置される。従って、制御要素により実行される機能は、多数の異なる装置間に分散することができる。

本発明によれば、比較器32は、セキュリティ機能を含み、そしてブロック28は、媒体アクセス制御(MAC)機能を含むことに注意されたい。

【0025】

図1の構造及び構成において、上述した特許出願に教示されたように、AP14、114と移動ターミナル12とで形成された通信対は、その通信対が両方とも所有権モードに適合しないと決定されたときにはIEEE802.11標準モードに準じて動作でき、或いはその通信対の両メンバーが所有権モード可能であると決定されたときには所有権モードに準じて動作できる。この結果を生じさせるために、比較器32は、通信対を形成する移動ターミナル及びアクセスポイントの両方の動作し得るモードを識別する識別子を受信する。次いで、モードセクタ34は、移動ターミナルとアクセスポイントとの間の通信のために標準的な動作モード又は所有権動作モードを選択する。

【0026】

移動ターミナル12の物理的な位置が所与の通信セッション中にセル18からセル118へ変化するときには、移動ターミナル12は、AP14によりサービ

スされる第1地理的エリア18を出て、AP114によってサービスされる第2地理的エリア118に入る。このセル対セル又はエリア対エリア移動は、第1エリア18に関連した古いAP14から、第2エリア118に関連した新たなAP114への通信のハンドオーバーを必要とし、これにより、移動ターミナル12との連続した通信が許される。

ハンドオーバー利用性決定装置36は、通信ハンドオーバーが可能である利用可能なAPの指示を移動ターミナル12に与え、この利用性は、通信ハンドオーバーに利用できるAPの認識を含む利用可能なアクセスポイントのリスト38に含まれる。

【0027】

利用可能なアクセスポイントのリスト38は、選択された時間間隔で移動ターミナル12に通信することもできるし、又はアクセスポイントのリスト38は、移動ターミナルが最初にアクチベートされるときに各移動ターミナル12に与えることもできるし、或いはネットワークプレフィックス又はネットワークプレフィックスのリストを使用して同じ目的を達成することもできる。

本発明のこの説明では、移動ターミナル12と、現在の又は古いAP14との間にセキュリティ関連性(SA)が存在すると仮定する。即ち、移動ターミナル12及びAP14は、同じ共通セットのキーと、セキュリティ機能を達成するのに必要な他の情報とを共有すると仮定する。本発明によれば、この確立されそして共有されるセキュリティ関連性が、移動ターミナルがセル18からセル118へ移動するときに機密形態で古いAP14から新たなAP114へ転送される。この転送は、転送を行うに必要なメッセージの数を最小にし、そしてパブリックキー暗号の使用を排除することにより、非常に迅速に行われる。その結果、移動ターミナル12への及びそこからのペイロードトラフィックの中断が最小にされ、この種の中断は、ボイス・オーバーIP(VOIP)及び映像配信のようなリアルタイムサービスにとって非常に重大である。

【0028】

本発明によれば、通信リンク(即ち移動ターミナル12及びAP14を伴うリンク)の両端に対する認証キー又はセキュリティ関連性は、IKEのようなシー

ル可能なキーマネジメントプロトコルによって発生され、ディフィー・ヘルマンのキー交換プロトコルも使用できることに注意されたい。

その後、移動ターミナル12がセル18及びそのAP14からセル118及びそのAP114へ移動するときに、ハンドオーバープロセス中の認証が本発明の簡単なチャレンジ/応答手順によって達成される。又、セキュリティ関連性は、古いAP14と新たなAP114との間に転送され、従って、古いAP14から新たなAP114へのハンドオーバー中に新たなキー交換を行う必要性が排除される。

【0029】

チャレンジ/応答手順の間に、新たなAP118は、移動ターミナル12へチャレンジを送信し、その際に、移動ターミナル12は、新たなAP118に応答を送信する。更に、移動ターミナル12は、新たなAP118をハンドオーバー中に同様に認証する。

キー及びそれに関連した情報が新たなAP114により要求され、その際に、それらは古いAP14から新たなAP114へハンドオーバーメッセージにおいて転送される。同様に、認証チャレンジの交換及びそれに対する応答は、新たなAP114と、移動ターミナル12との間に生じるハンドオーバーシグナリングに一体化される。

【0030】

図2は、本発明による順方向ハンドオーバー（HO）プロセス20を示し、これは、本発明の好ましい実施形態である。順方向ハンドオーバープロセス20では、移動ターミナル（MT又はmt）と新たなアクセスポイント（AP又はap）114との間にハンドオーバーシグナリングが送信される。この形式のハンドオーバーは、特に、無線リンク21が事前の警告なしに失われるときに特に有用である。

図3は、本発明による逆方向ハンドオーバー（HO）プロセス30を示す。逆方向ハンドオーバープロセス30においては、古いAP14と通信する移動ターミナル12によってハンドオーバーが要求され、その結果、図2に示したものと若干異なるメッセージシーケンスが生じる。逆方向ハンドオーバー中の有益な

オプションは、古いAP 14から移動ターミナル12へ認証チャレンジを搬送する無線インターフェースメッセージ31を使用して、逆方向ハンドオーバー33もトリガーすることである。即ち、古いAP 14から切断しそしてセキュリティ関連性(SA) 35が移動ターミナル12に対して既に準備された新たなAP 114へ接続すべきであることを移動ターミナル12に指示するために、認証チャレンジ31が使用される。

【0031】

ここで使用される「古いAP」という語は、移動ターミナル12が最初に又は現在通信しているアクセスポイント14のようなアクセスポイントを意味する。従って、「古いAP」という語は、通信ハンドオーバーが必要とされる時点で移動ターミナル12が通信している「現在AP」も意味する。

ここで使用する「新たなAP」という語は、移動ターミナル12が古いセル18から新たなセル118へ地理的に移動したために移動ターミナル12が通信を開始しなければならないアクセスポイント114のようなアクセスポイントを意味する。従って、「新たなAP」という語は、通信ハンドオーバーが完了した後に移動ターミナル12が通信する「将来のAP」も意味する。

【0032】

図2及び3には、IEEE 802.11メッセージ名が使用され、そしてハンドオーバーメッセージの付加的なパラメータが示されている。しかしながら、このメッセージ名は、本発明の範囲にとって重要ではない。というのは、本発明は、IEEE 802.11以外のシステムでも実施できるからである。しかしながら、図2及び3の拡張MAC（媒体アクセス制御）メッセージを使用して、無線インターフェースを経て付加的なパラメータを搬送することは、付加的なメッセージを送信する必要性が排除されるという点で有益である。

セキュリティを保証するためには、キーを搬送するメッセージを暗号化するのが望ましい。それ故、AP 14、114間でのセキュリティ関連性即ちSA及び他の制御トラフィックの転送は、IPsecにより暗号化されそして認証されるものとして示されている。

【0033】

従って、ハンドオーバーが必要とされるように移動ターミナル12がセル18、118に対して物理的に移動されたことを決定する特定の手段は、本発明にとって重要ではない。例えば、その手順は、移動支援ハンドオーバー手順を使用する従来の時分割セルラーシステムに使用されるものと同様でよい。一般に、移動ターミナル12は、セル18、118のような隣接セルのベースステーション又はAPの制御チャンネルに、例えば、タイミングを合わせた間隔で同調する。次いで、これらの制御チャンネルにブロードキャストされる信号の信号強度、又はビットエラー率のような他の信号特性が移動ターミナル12により測定され又は感知される。移動ターミナル12におけるこの測定をベースとするアップリンク信号は、次いで、移動ターミナルによりネットワーク10へ送信され、その際に、ネットワーク10は、通信ハンドオーバーを行うべきかどうか決定する。ハンドオーバーが必要であると決定された場合には、命令が移動ターミナル12に送信され、そして図2又は3の通信ハンドオーバープロセスが開始される。

【0034】

図4Aないし4Cは、移動ターミナル12がセル18からセル118へ移動するときに移動ターミナル12の通信ハンドオーバーが古いAP14及び新たなAP114に対して行われる順方向ハンドオーバープロセス20を示す別の図である。この図において、移動ターミナル即ちMTは、「mt」とも称され、そしてアクセスポイント即ちAPは、「ap」とも称される。

図4Aを参照すれば、順方向ハンドオーバープロセス20は、ハンドオーバーが要求されることを指示する事象401のイエス出力400により移動ターミナル12において開始される。移動ターミナル12は、ここで、ファンクション402において、無線ハンドオーバー機能をアクチベートするように動作する。

ファンクション403において、移動ターミナル12は、新たなAP114へチャレンジを発生し、その際に、ファンクション404において、「mt_challenge」を含むMAC_REASSOCIATE_REQメッセージが新たなAP114へ送信される。

【0035】

ファンクション405において、新たなAP114は、メッセージ404を受

け入れ、その際に、新たなAP114は、ファンクション406において、ハンドオーバー要求を古いAP14へ送信するように動作する。

古いAP14は、ここで、ファンクション407において、セキュリティ関連性パラメータSA、SAをそのセキュリティ関連性データベースから検索するように動作する。次いで、古いAP14は、ファンクション408において、パラメータSA、SAを含むハンドオーバー要求を新たなAP114へ送信するように動作する。

図4Bを参照すれば、新たなAP114は、ここで、ファンクション409においてセキュリティ関連性(SA)を形成するように動作し、ファンクション410において移動ターミナル12を認証するためのチャレンジを発生するように動作し、ファンクション411において、図4Aのメッセージ404に含まれた「mt_challenge」に対する応答を計算するように動作し、そしてファンクション412において、MAC_AUTHENTICATE_REQメッセージを移動ターミナル12へ送信するように動作する。メッセージ412は、ファンクション411の動作により計算された「ap_response」を含み、ファンクション410の動作により発生された「ap_challenge」を含み、そして「他の情報」を含む。

【0036】

移動ターミナル12は、ここで、ファンクション413においてそのセキュリティ関連性パラメータを更新するように動作し、ファンクション414においてメッセージ412により受け取られた「ap_challenge」に対する応答を計算するように動作し、そしてファンクション415において、メッセージ412により受け取られた「ap_response」を正しい又は予想される応答と比較するように動作する。

ファンクション415により実行された比較が正しい比較を生じた場合には、ファンクション416は、新たなAP114を認証するように動作し、その際に、ファンクション417は、MAC_AUTHENTICATE_RESPメッセージを新たなAP114へ送信するように動作し、このメッセージは、ファンクション414で計算された「mt_response」を含む。

【0037】

図4Cを参照すれば、ファンクション418において、新たなAP114は、メッセージ417により受け取られた「mt_response」を適切な又は正しい応答と比較するように動作し、そしてこの比較が正しい比較を生じるときには、ファンクション419が移動ターミナル12を認証するように動作する。新たなAP114は、次いで、ファンクション420において、MAC_REASSOCIATE_RESPメッセージを移動ターミナル12へ送信するように動作し、その際に、ハンドオーバーが完了し、そしてその後、移動ターミナル12は、ファンクション421において、新たなAP114を使用してそのペイロードトラフィックを再開するように動作する。

図5Aないし5Cは、通信ハンドオーバーが移動ターミナル12について古いAP14及び新たなAP114に対して行われる逆方向ハンドオーバープロセス30を示す別の図である。この図では、移動ターミナル即ちMTが「mt」とも称され、そしてアクセスポイント即ちAPが「ap」とも称される。

【0038】

図5Aを参照すれば、ハンドオーバーが要求されたことを指示する事象501のイエス出力500により逆方向ハンドオーバープロセス30が移動ターミナル12において開始される。移動ターミナル12は、ここで、ファンクション502においてハンドオーバー要求を古いAP14へ送信するように動作する。

メッセージ502が古いAP14に受け取られると、ファンクション503はそのメッセージを受け入れ、ファンクション504は、セキュリティ関連性パラメータSA、SAをそのセキュリティ関連性(SA)データベースから検索するように動作し、そしてファンクション505は、パラメータSA、SAを含むハンドオーバー要求を新たなAP114へ送信するように動作する。

【0039】

メッセージ505で受け取られたパラメータSA、SAを使用して、新たなAP114は、ここで、ファンクション506において、それ自身のセキュリティ関連性(SA)を生成するように動作する。新たなAP114は、次いで、ファンクション507において、移動ターミナル12を認証するためのチャレンジを

発生するように動作し、そしてファンクション508において、ハンドオーバー要求が古いAP14へ送信され、この要求508は、ファンクション507で発生された「ap_challenge」及び「他の情報」を含む。

図5Bを参照すれば、メッセージ508に応答して、古いAP14は、ファンクション509において、MAC_DISSOCIATEメッセージを移動ターミナル12へ送信するように動作し、このメッセージは、古いAP14がメッセージ508により新たなAP114から受信した「ap_challenge」及び「他の情報」を含んでいる。

【0040】

メッセージ509に応答して、移動ターミナル12は、その無線ハンドオーバーファンクションを510においてアクチベートする。ファンクション511において、移動ターミナル12は、ここで、そのセキュリティ関連性パラメータを更新し、ファンクション512において、移動ターミナル12は、メッセージ508及び509の「ap_challenge」に対する応答を計算するように動作し、ファンクション513において、移動ターミナル12は、新たなAP114を認証するためのチャレンジを発生するように動作し、そしてファンクション514において、移動ターミナル12は、MAC_REASSOCIATE_REQメッセージを新たなAP114へ送信するように動作する。メッセージ514は、ファンクション511で計算された「mt_response」、ファンクション512で発生された「mt_challenge」及び「他の情報」を含む。

【0041】

図5Cを参照すれば、ファンクション515は、移動ターミナル12の認証を与え、ファンクション516は、メッセージ513により受け取られた「mt_response」を正しい又は予想応答と比較し、ファンクション517は、メッセージ513により受け取られた「mt_challenge」に対する応答を計算し、そしてファンクション518は、MAC_REASSOCIATE_RESPメッセージを移動ターミナル12に送信するように動作し、メッセージ518は、ファンクション517により計算された「ap_resp

onse」を含んでいる。

ファンクション519において、移動ターミナル12は、新たなAP114を認証するように動作し、これは、ファンクション520において、メッセージ518に含まれた「ap_response」を正しい又は予想応答と比較することで行われ、その正しい比較の結果として、ファンクション521は、移動ターミナル12が新たなAP114を使用してペイロードトラフィックを再開するようにさせる。

【0042】

以上のことから明らかなように、本発明は、所定の移動ターミナル12との通信が第1アクセスポイント14から第2アクセスポイント114へハンドオーバーされるときに情報のセキュリティを与える方法及び装置を提供する。複数のアクセスポイントを有する通信システム10が設けられ、各アクセスポイントは、通信システム10によりサービスされる全地理的エリア内の異なる地理的エリアにサービスし、そして複数の移動ターミナル12が設けられ、これら移動ターミナルは、全地理的エリア内及び異なる地理的エリア間を個々に物理的に移動することができる。

本発明のハンドオーバープロセス／装置において、最初に、所与の移動ターミナル12が、第1アクセスポイント14との通信作用から、第2アクセスポイント114との通信作用へと移動するときに、それが感知される（図4Aの401及び図5Aの501を参照）。

【0043】

このような移動が感知されると、セキュリティ関連性パラメータが第1アクセスポイント14からフェッチされ（図4Aの407及び図5Aの504を参照）、その検索されたセキュリティ関連性パラメータに基づき第2のアクセスポイント114においてセキュリティ関連性が生成され（図4Bの409及び図5Aの506を参照）、そしてその検索されたセキュリティ関連性パラメータに基づき所与の移動ターミナル12においてセキュリティ関連性が生成される（図4Bの413及び図5Bの510を参照）。

又、このような移動が感知されると、所与の移動ターミナル12から第2のA

クセスポイント114へ認証アクセスポイントチャレンジが送信され(図4Aの404及び図5Bの513を参照)、そして第2のアクセスポイント114から所与の移動ターミナル12へ認証移動ターミナルチャレンジが送信される(図4Bの412及び図5Aの508を参照)。上記アクセスポイントチャレンジは、本発明の任意の特徴であることに注意されたい。

【0044】

所与の移動ターミナル12から受け取られた認証アクセスポイントチャレンジに応答して、第2アクセスポイント114は、ここで、認証アクセスポイント応答を発生し(図4Bの411及び図5Cの516を参照)、そしてこの認証アクセスポイント応答は、所与の移動ターミナル12へ送信される(図4Bの412及び図5Cの517を参照)。

第2アクセスポイント114から受け取られた認証移動ターミナルチャレンジに応答して、所与の移動ターミナル12は、ここで、認証移動ターミナル応答を計算し(図4Bの414及び図5Bの511を参照)、そしてこの認証移動ターミナル応答は、第2アクセスポイント114へ送信される(図4Bの417及び図5Bの513を参照)。

【0045】

所与の移動ターミナル12における第1比較は、ここで、第2アクセスポイント114から受け取られた認証アクセスポイント応答を、正しい又は予想応答と比較するように動作し(図4Bの415及び図5Cの519を参照)、そして第2アクセスポイント114における第2比較は、ここで、所与の移動ターミナル12から受け取った認証移動ターミナル応答を、正しいまたは予想応答と比較するように動作する(図4Cの418及び図5Cの515を参照)。

最終的に、第1比較及び第2比較の結果に基づいて所与の移動ターミナル12と第2アクセスポイント114との間で通信が開始される(図4Cの421及び図5Cの520を参照)。

【0046】

図6及び7は、本発明の2つの付加的な実施形態を示す。図6及び7の実施形態は、その特定の細部が相違するが、図6及び7の実施形態の内容は、本発明の

上記図2、3、4A-4B及び5A-5Bと比較することにより容易に明らかとなろう。

以上、本発明の好ましい実施形態を詳細に説明したが、これは、本発明の精神及び範囲を何ら限定するものではなく、当業者であれば、特許請求の範囲に規定された本発明の範囲内で他の実施形態が容易に明らかとなろう。

【図面の簡単な説明】

【図1】

本発明の実施形態が作用する通信システムを示す図である。

【図2】

本発明による順方向ハンドオーバープロセスを示す図である。

【図3】

本発明による逆方向ハンドオーバープロセスを示す図である。

【図4A】

図2の順方向ハンドオーバープロセスを示す別の図である。

【図4B】

図2の順方向ハンドオーバープロセスを示す別の図である。

【図4C】

図2の順方向ハンドオーバープロセスを示す別の図である。

【図5A】

図3の逆方向ハンドオーバープロセスを示す別の図である。

【図5B】

図3の逆方向ハンドオーバープロセスを示す別の図である。

【図5C】

図3の逆方向ハンドオーバープロセスを示す別の図である。

【図6】

本発明によるH I P E R L A N / 2 強制ハンドオーバーを示す図である。

【図7】

本発明によるH I P E R L A N / 2 順方向ハンドオーバーを示す図である。

【図1】

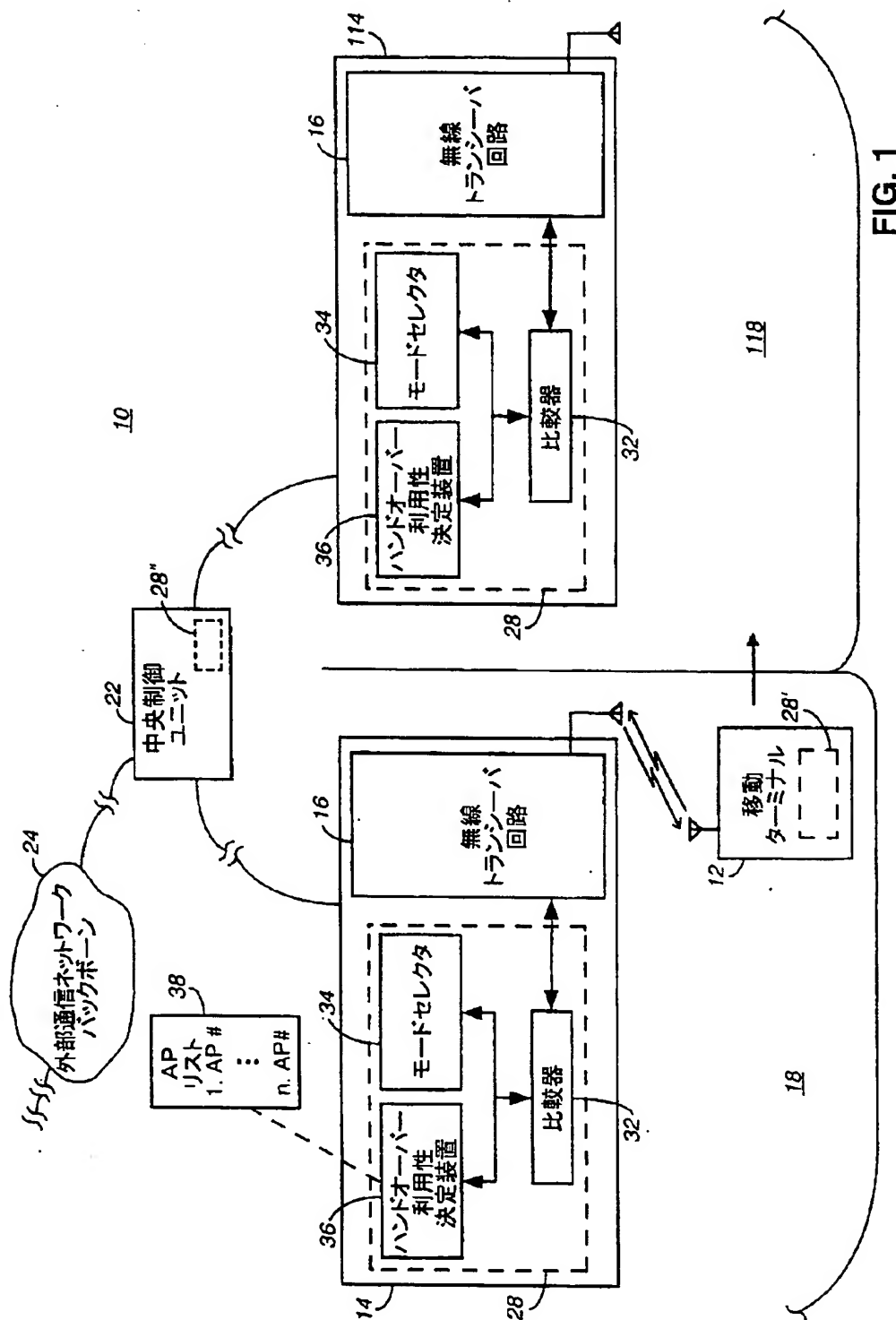


FIG. 1

【図2】

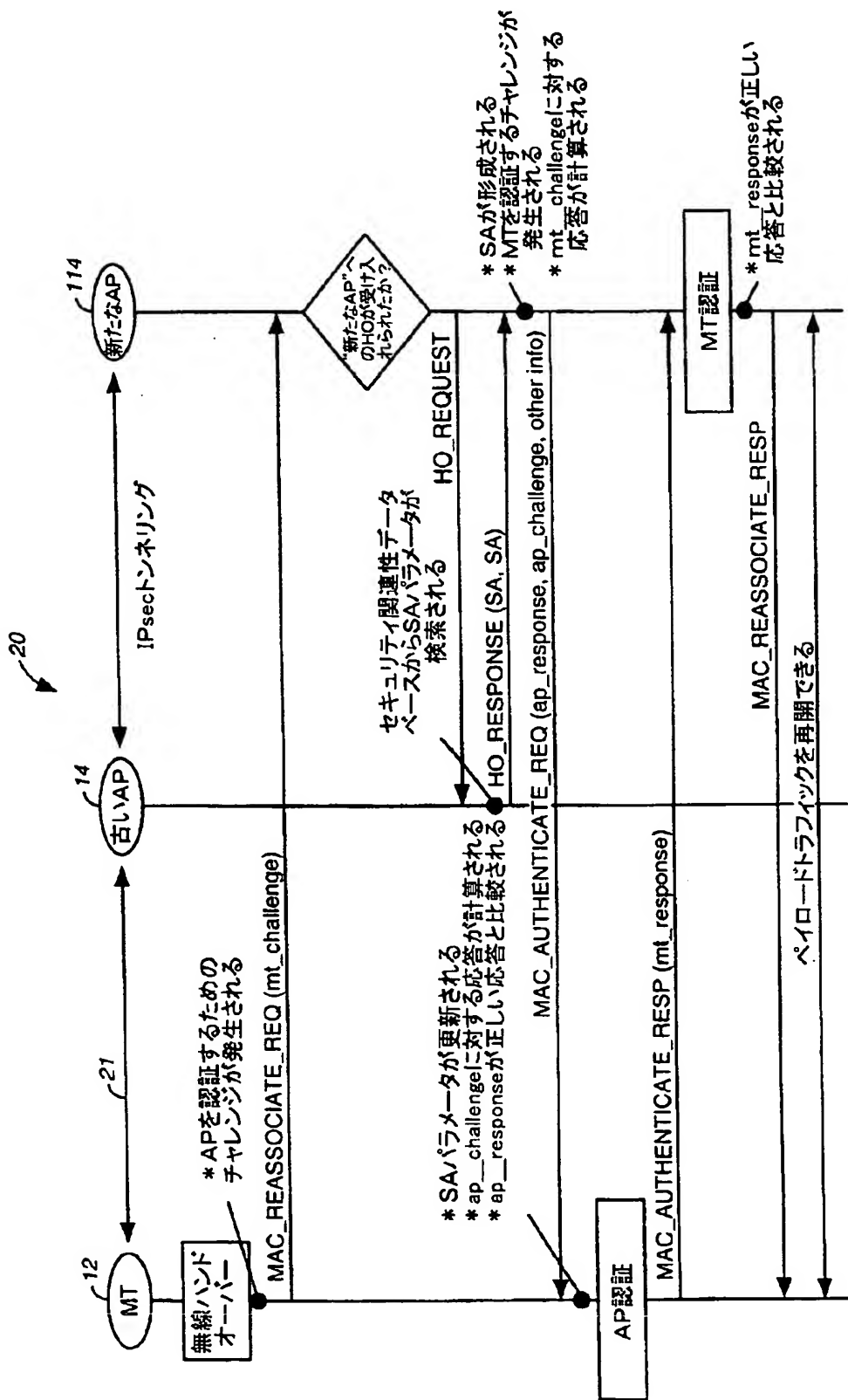


FIG. 2

【図 3】

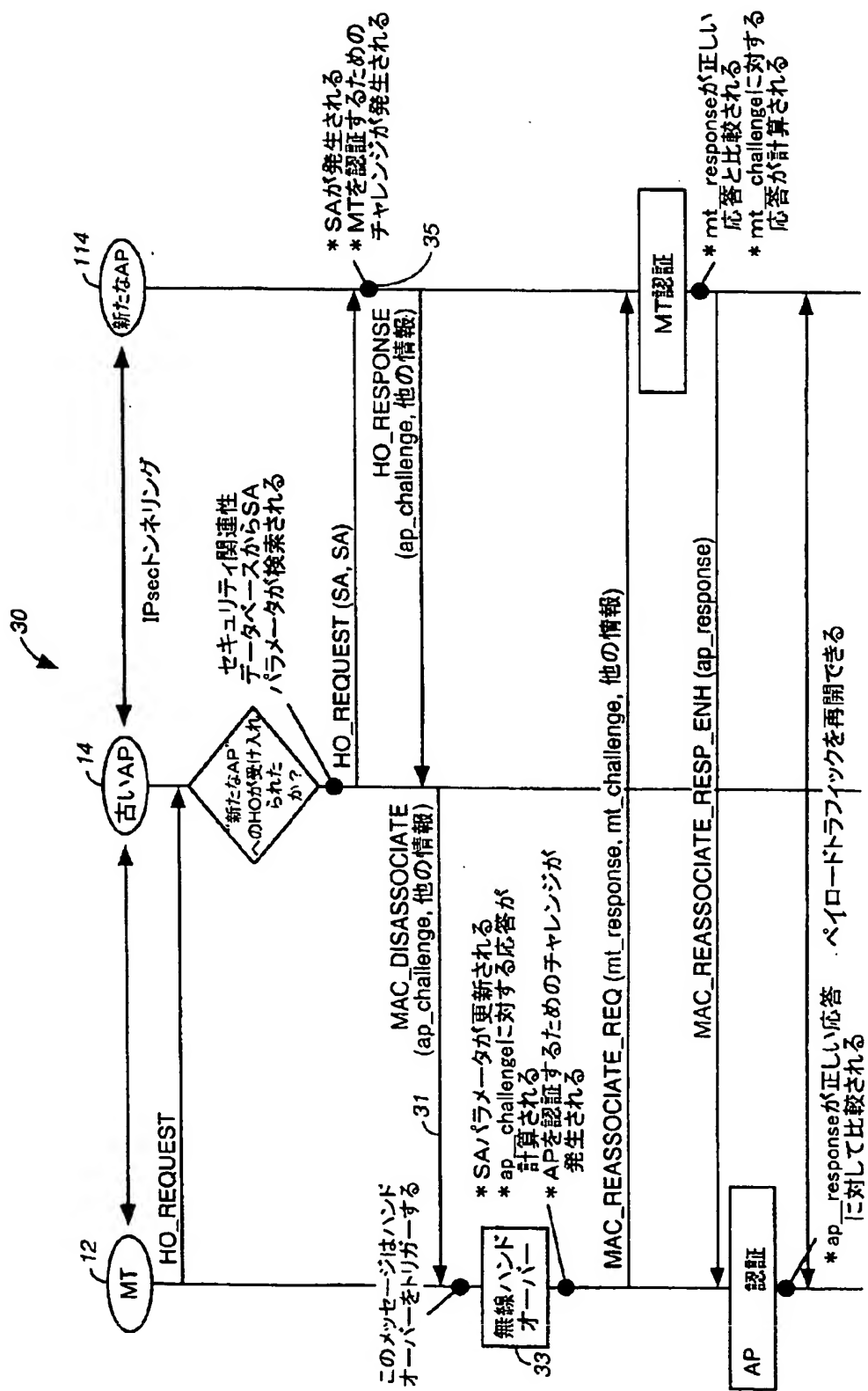


FIG. 3

【図4A】

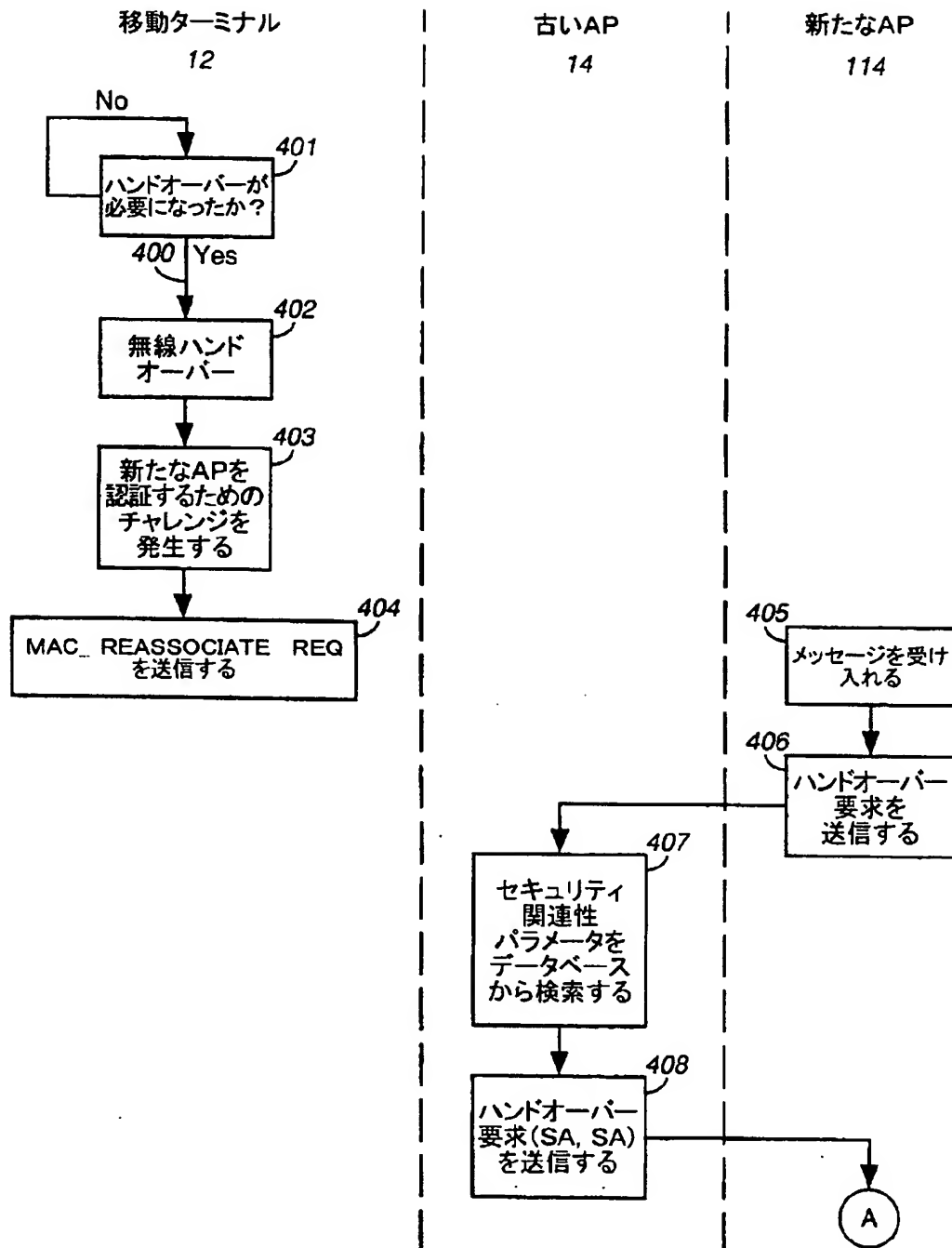


FIG. 4A

【図4B】

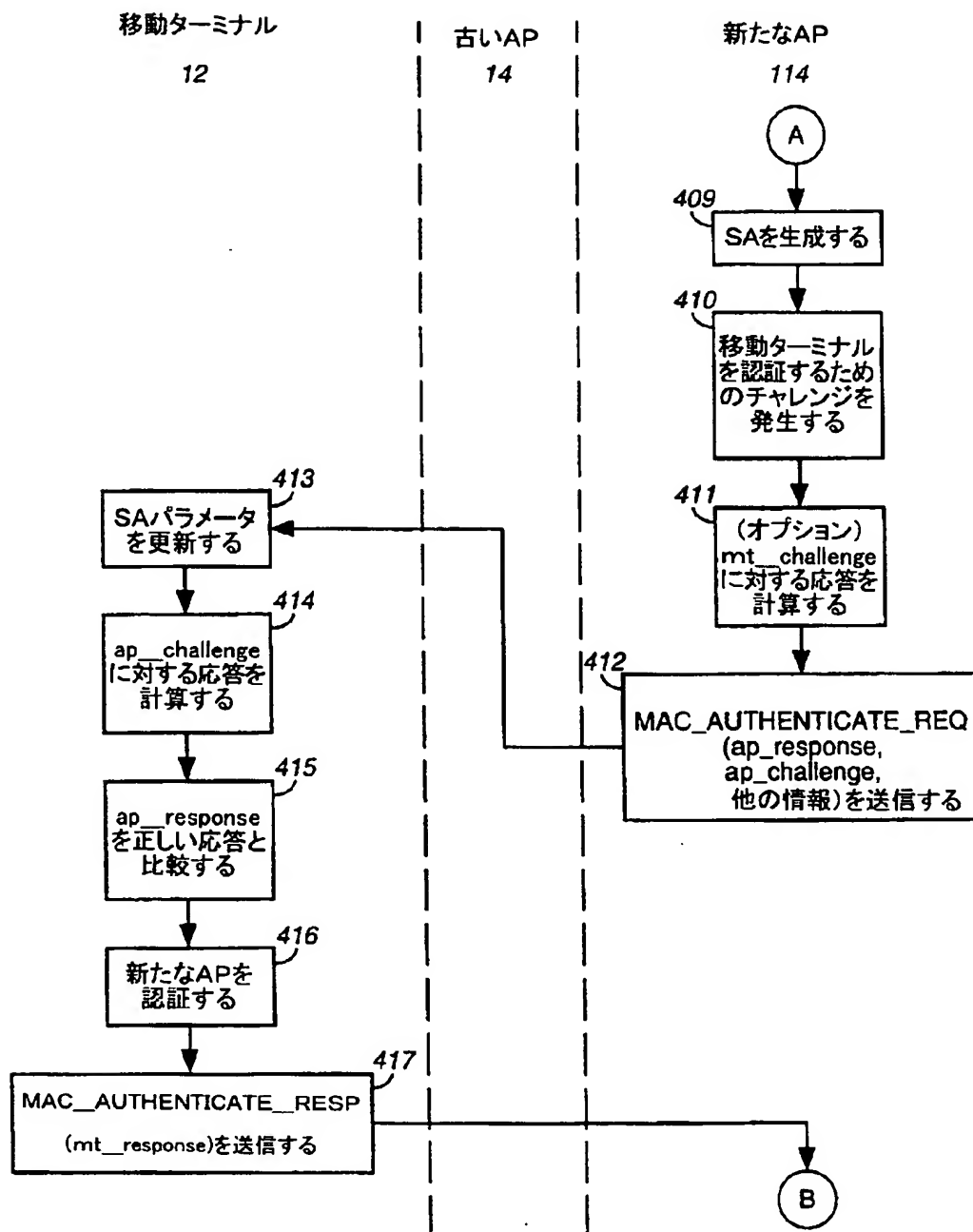


FIG. 4B

【図4C】

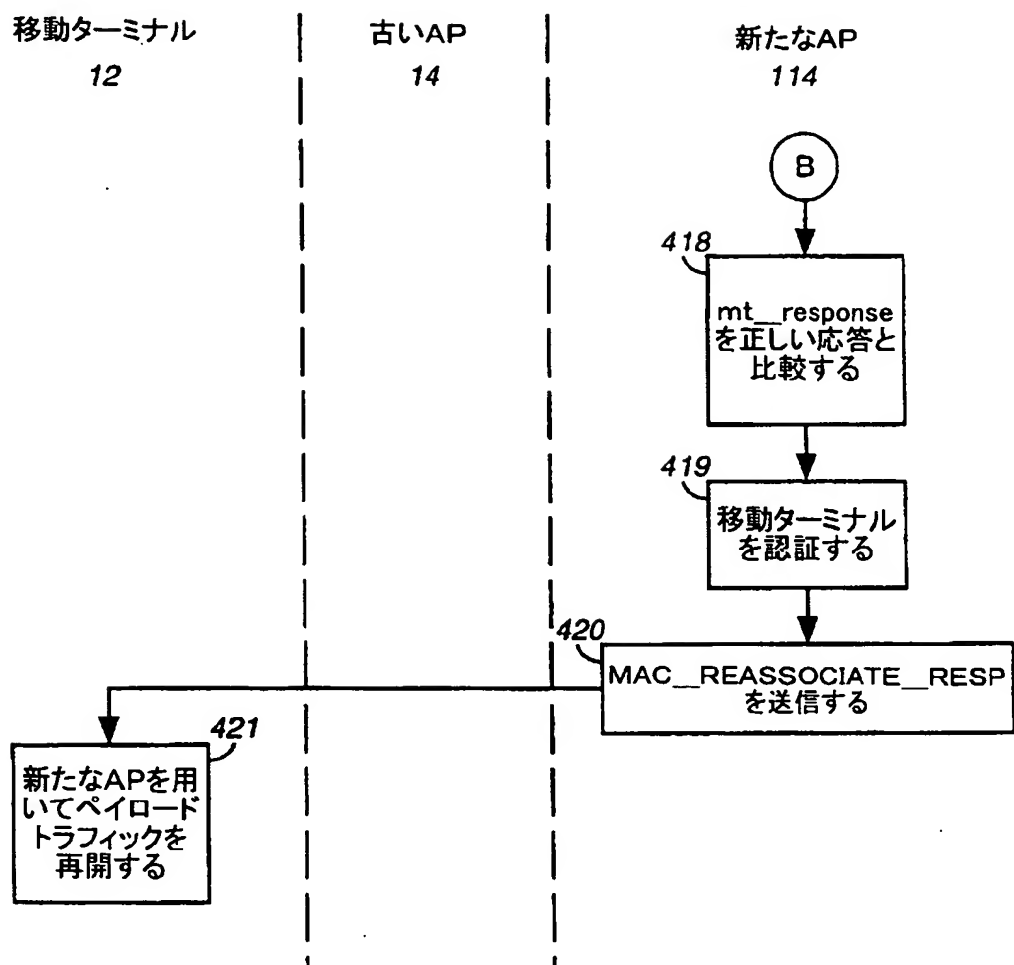


FIG. 4C

【図5A】

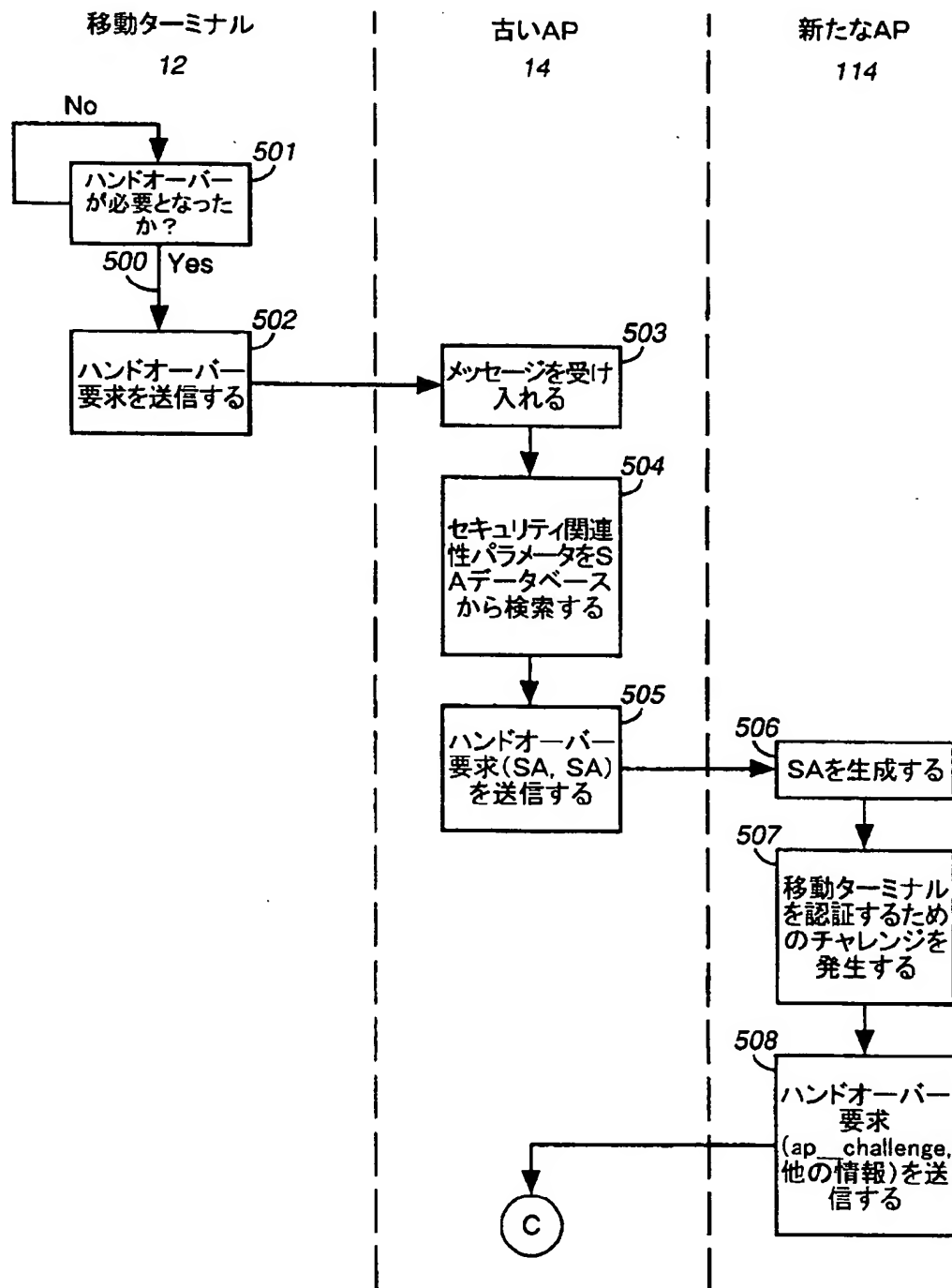


FIG. 5A

【図5B】

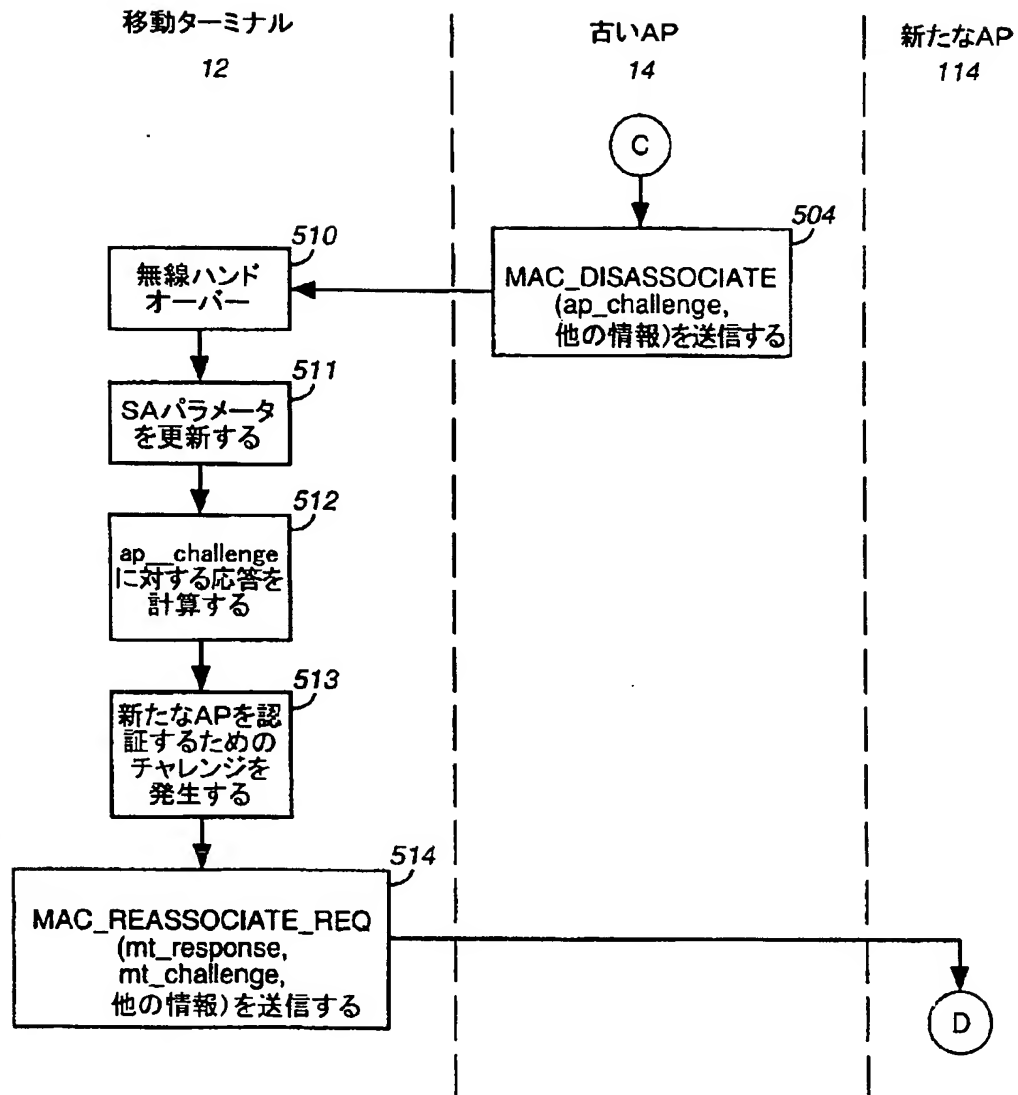


FIG. 5B

【図5C】

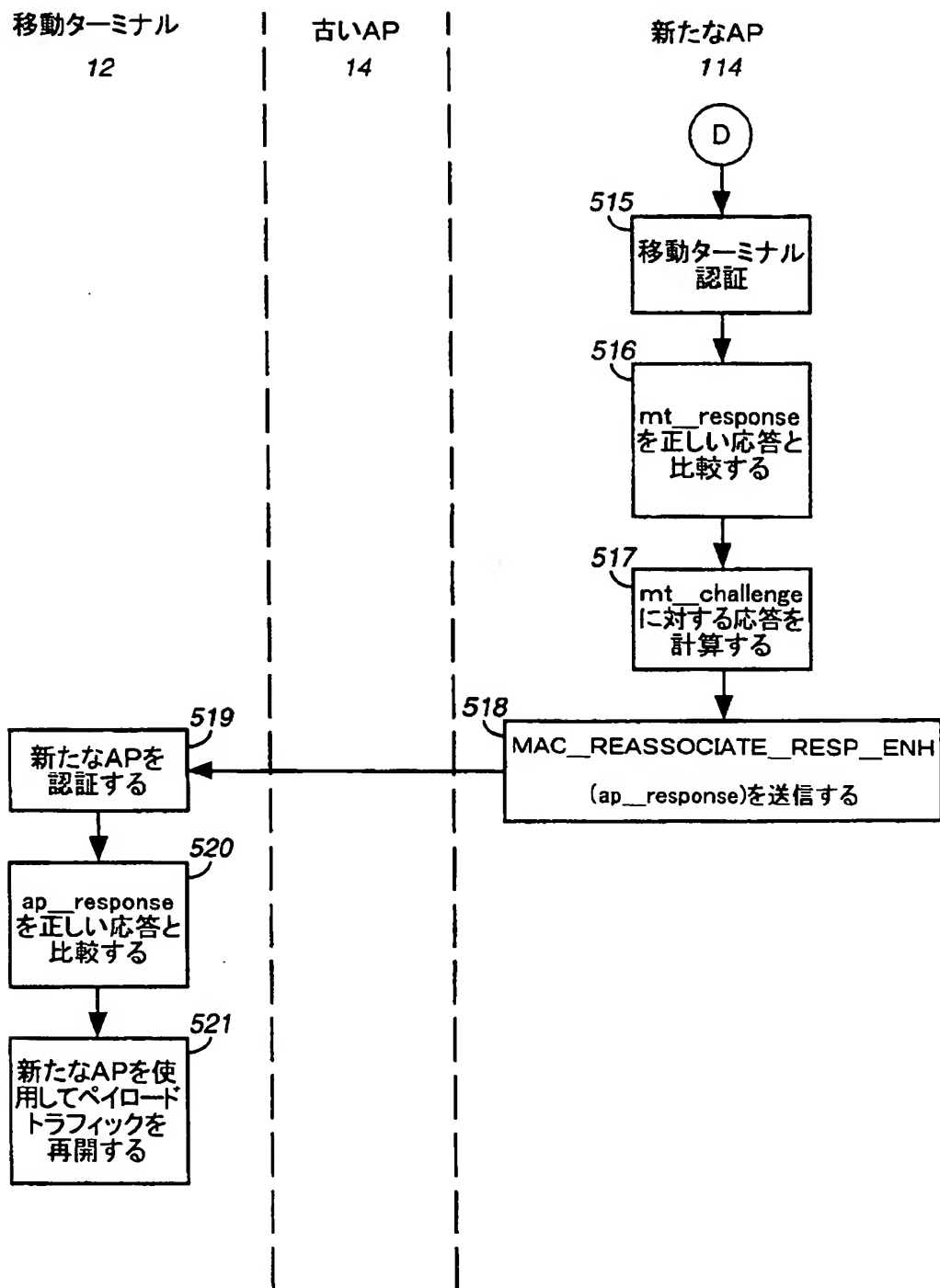


FIG. 5C

【図6】

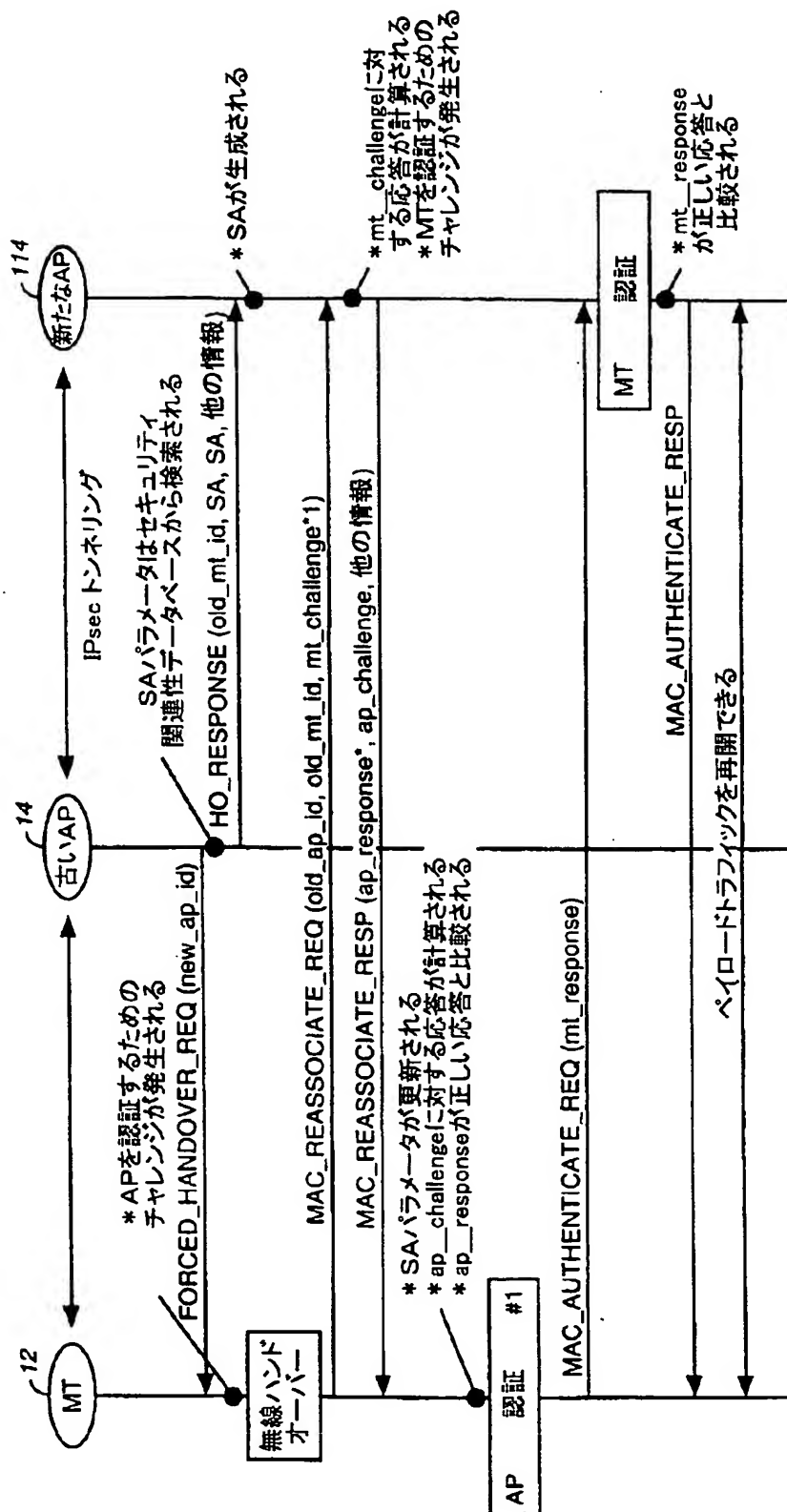


FIG. 6

【図7】

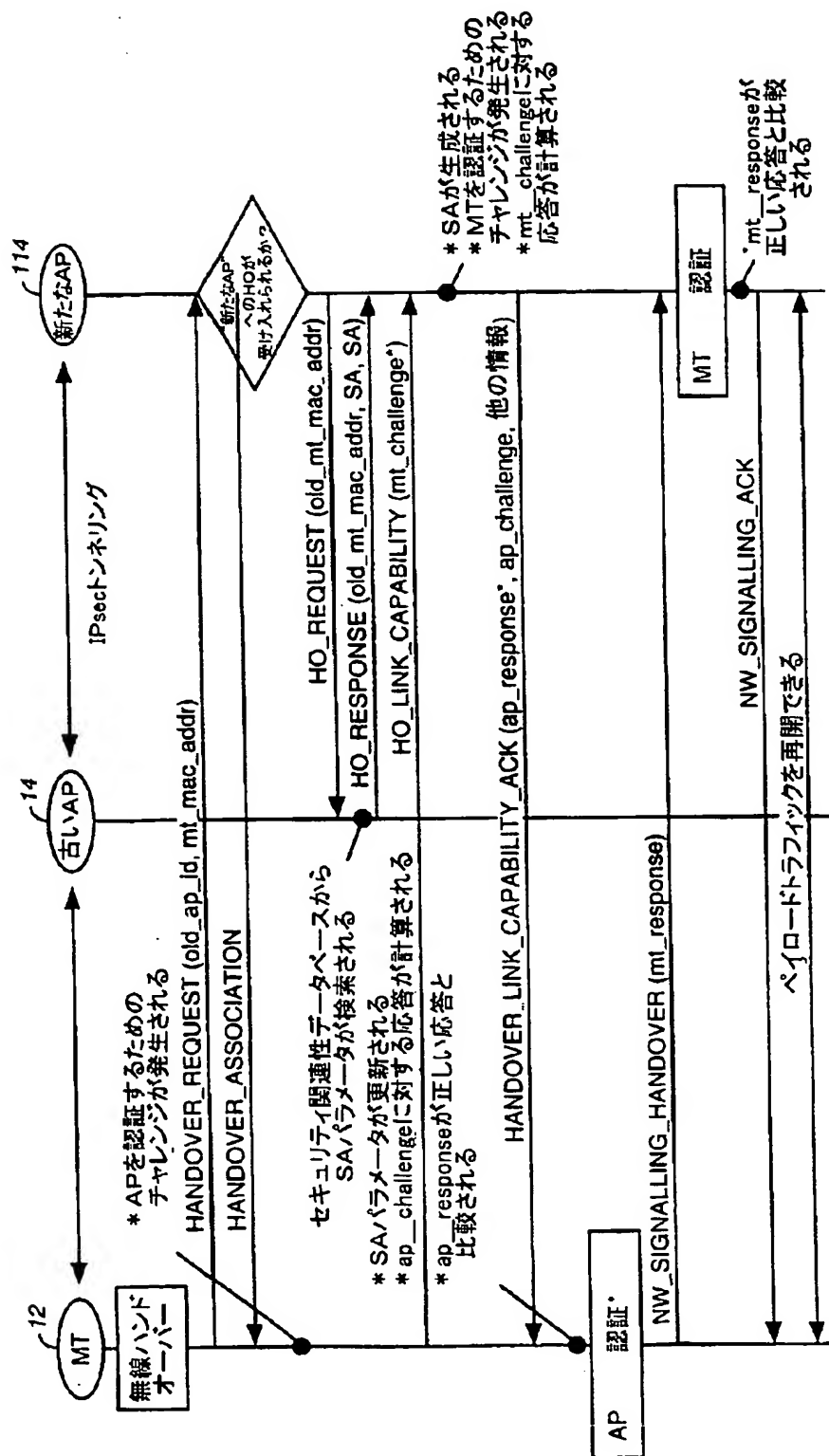


FIG. 7

【手続補正書】特許協力条約第34条補正の翻訳文提出書

【提出日】平成13年10月9日(2001.10.9)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】 所定の移動ターミナル(12)との通信が第1アクセスポイント(14)から第2アクセスポイント(114)へハンドオーバーされるときに情報セキュリティを与える方法(20)において、

複数のアクセスポイント(14, 114)を有する通信システム(10)を用意し、各アクセスポイントは、上記通信システムによりサービスされる全地理的エリア内の異なる地理的エリア(18, 118)にサービスし、

上記全地理的エリア内で上記異なる地理的エリア(18, 118)間を各々物理的に移動可能な複数の移動ターミナル(12)を用意し、

上記所定の移動ターミナルが上記第1アクセスポイントとの通信作用から上記第2アクセスポイントとの通信作用へ移動するときを感知し(401)、

上記感知段階に応答して、上記第1アクセスポイント(14)からセキュリティ関連性パラメータを検索し(407)、その検索されたセキュリティ関連性パラメータに基づき上記第2アクセスポイント(114)にセキュリティ関連性を形成し(409)、そしてその検索されたセキュリティ関連性パラメータに基づいて上記所定の移動ターミナル(12)にセキュリティ関連性を形成し、そして

上記応答段階に基づいて上記所定の移動ターミナル(12)と上記第2アクセスポイント(114)との間に通信を開始する(421)、という段階を備えた方法。

【請求項2】 上記の感知段階(401)に応答して、上記所定の移動ターミナル(12)から上記第2アクセスポイント(114)へ認証アクセスポイントチャレンジ(412)を送信し(404)、そして上記第2アクセスポイント(114)から上記所定の移動

ターミナル(12)へ認証移動ターミナルチャレンジを送信し(412)、

上記所定の移動ターミナル(12)から受け取った上記認証アクセスポイントチャレンジに応答して上記第2アクセスポイント(114)に認証アクセスポイント応答を発生し(410)、

上記認証アクセスポイント応答を上記所定の移動ターミナルへ送信し(412)、

上記第2アクセスポイントから受け取った上記認証移動ターミナルチャレンジに応答して上記所定の移動ターミナル(12)に認証移動ターミナル応答を発生し(414)、

上記認証移動ターミナル応答を上記第2アクセスポイントへ送信し(417)、

上記認証アクセスポイント応答を上記所定の移動ターミナルにおいて正しい応答と第1比較し(415)、

上記認証移動ターミナル応答を上記第2アクセスポイントにおいて正しい応答と第2比較し(418)、そして

上記第1比較段階及び上記第2比較段階に基づいて上記所定の移動ターミナルと上記第2アクセスポイントとの間に通信を開始する(420)、
段階を更に備えた請求項1に記載の方法(20)。

【請求項3】 上記複数の移動ターミナル(12)は、媒体アクセス制御層及び互換性物理層を有し、そして上記メッセージは、媒体アクセス制御メッセージである請求項2に記載の方法(20)。

【請求項4】 上記メッセージは、ワイヤレスLAN内に送信され、IEEE 802.11又はHIPERLAN/2マルチアクセスメッセージである請求項3に記載の方法(20)。

【請求項5】 上記通信システム(10)は、セキュリティプロトコルを使用してデータパケットの端一端セキュリティを与えるWLAN通信システムである請求項2に記載の方法(20)。

【請求項6】 上記端一端セキュリティは、上記データパケットを認証及び／又は暗号化することにより与えられ、そして上記セキュリティプロトコルは、通信リンクの両端で同じ暗号及び／又は認証キーの使用を必要とする対称的暗号を与える請求項5に記載の方法(20)。

【請求項7】 シール可能なキー管理プロトコルは、上記セキュリティプロトコルに対する対称的キーを発生するよう動作する請求項6に記載の方法(20)。

【請求項8】 上記所定の移動ターミナルと上記第2のアクセスポイントとの間にセッション従属動的暗号化キーを与え、そして

上記通信システムにより与えられる通信カバレッジ内で上記所定の移動ターミナルが移動するときに第1アクセスポイントから第2アクセスポイントへアクティブなセキュリティ関連性を転送する、

という段階を備えた請求項6に記載の方法(20)。

【請求項9】 上記通信システム(10)をLANとして用意し、

上記LAN内にサーバーを用意し、

通信ハンドオーバー中に通信が続くときに、端一端セキュリティ関連性に変更を必要とせずに、通信ハンドオーバー中に上記LAN内にキー管理及びセキュリティ関連性再確立を与え、上記通信ハンドオーバーが上記移動ターミナルと上記第1及び第2アクセスポイントとの間のセキュリティ機能にしか影響しないようにする、

という段階を備えた請求項4に記載の方法(20)。

【請求項10】 上記LANは、上記複数のアクセスポイント(14, 114)と上記複数の移動ターミナル(12)との間にインターネットプロトコルセキュリティベースのセキュリティ関連性を含む請求項9に記載の方法(20)。

【請求項11】 上記所定の移動ターミナル(12)及び上記第1及び第2のアクセスポイント(14, 114)で作られた通信対の両端に対して認証キーが与えられ、この認証キーは、スケーリング可能なキー管理プロトコルにより発生される請求項1に記載の方法(20)。

【請求項12】 上記所定の移動ターミナル(12)と上記第1アクセスポイント(14)の間にはスケーリング可能なキー管理プロトコルに基づいて認証キー又はセキュリティ関連性が存在し、そして通信ハンドオーバー中に新たなキー交換の必要性を回避するために上記複数のアクセスポイント(14, 114)間にセキュリティ関連性が転送される請求項1に記載の方法(20)。

【請求項13】 上記スケーリング可能なキー管理プロトコルは、IKEで

あり、そして上記第1アクセスポイント(14)から上記第2アクセスポイント(114)への上記通信ハンドオーバー中に新たなキー交換の必要性を回避するやり方で上記第1アクセスポイント(14)と上記第2アクセスポイント(114)との間にセキュリティ関連性が転送される請求項12に記載の方法(20)。

【請求項14】 キーを搬送するメッセージを暗号化する段階を含む請求項13に記載の方法(20)。

【請求項15】 第1通信アクセスポイント(14)によりサービスされる第1地理的エリア(18)から、第2通信アクセスポイント(114)によりサービスされる第2地理的エリア(118)へ移動ターミナル(12)が物理的に移動するときに通信ハンドオーバーが発生するとき無線通信システム(10)に所定のセキュリティ関連性を維持するための装置であって、上記移動ターミナル(12)は、最初に、上記第1通信アクセスポイント(14)と第1通信対を形成し、そして上記通信ハンドオーバーの後に、上記移動ターミナルは、上記第2通信アクセスポイント(114)と第2通信対を形成し、上記第1通信対(12-14)の各メンバーは、それに関連した上記所定のセキュリティ関連性を有し、上記装置は、

上記移動ターミナル(12)にあつて上記通信ハンドオーバーを開始する必要性を感知するための第1手段(40)と、

上記無線通信システム(10)内にあつて、上記第1手段(40)が上記通信ハンドオーバーを開始する上記必要性を感知するのに応答して、上記第2通信アクセスポイント(114)に上記所定のセキュリティ関連性を確立するための第2手段(405)と

上記移動ターミナル(12)にあつて、上記所定のセキュリティ関連性の関数としてアクセスポイントチャレンジを発生し、そしてそのアクセスポイントチャレンジを上記第2通信アクセスポイントへ送信するための第3手段(403)と、

上記第2通信アクセスポイントにあつて、上記第2通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数として移動ターミナルチャレンジを発生し、そしてその移動ターミナルチャレンジを上記移動ターミナルへ送信するための第4手段(410)と、

上記移動ターミナルにあつて、上記移動ターミナルチャレンジに応答して、上

記所定のセキュリティ関連性の関数として移動ターミナル応答を発生し、そしてその移動ターミナル応答を上記第2通信アクセスポイントへ送信するための第5手段(414)と、

上記第2通信アクセスポイントにあつて、上記アクセスポイントチャレンジに応答して、上記第2通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数としてアクセスポイント応答を発生し、そしてそのアクセスポイント応答を上記移動ターミナルへ送信するための第6手段(409)と、

上記移動ターミナルにあつて、上記アクセスポイント応答に応答して、上記アクセスポイント応答が上記所定のセキュリティ関連性の関数として正しいかどうか決定するための第7手段と、

上記第2通信アクセスポイント(114)にあつて、上記移動ターミナル応答に応答して、上記移動ターミナル応答が、上記第2通信アクセスポイントに確立された上記所定のセキュリティ関連性の関数として正しいかどうか決定するための第8手段(418)と、

上記無線通信システム(10)内にあつて、上記第8及び第9手段に応答して、上記移動ターミナル応答及び上記アクセスポイント応答の両方が正しいときに上記通信ハンドオーバーを確立するための第9手段(420)と、
を備えた装置。

【請求項16】 上記無線通信システム(10)は、グループIEEE802.11及びHIPERLANから選択される請求項15に記載の装置。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Intern. Appl. No.
PCT/IB 00/01713

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 939 519 A (NO WIRES NEEDED B V) 1 September 1999 (1999-09-01) column 4, line 8 - line 58 figure 1	15,18,20
A	US 5 778 075 A (HAARTSEN JACOBUS CORNELIS) 7 July 1998 (1998-07-07) column 4, line 24 - line 50 column 9, line 43 - line 60 column 18, line 15 - line 60 figures 5,13	1
P,X	WO 00 49827 A (ERICSSON TELEFON AB L M) 24 August 2000 (2000-08-24) page 2, line 20 -page 5, line 25 figure 2	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *A* document member of the same patent family

Date of the actual completion of the international search

3 April 2001

Date of mailing of the international search report

11/04/2001

Name and mailing address of the ISA
European Patent Office, P.O. Box 5018 Patentkan 2
NL - 2220 HY Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 eponit
Fax: (+31-70) 340-3016

Authorized officer

Barel, C

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern. Appl. No.
PCT/IB 00/01713

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0939519	A	01-09-1999	NL 1008351 C	20-08-1999
US 5778075	A	07-07-1998	AU 3875797 A	19-03-1998
			NO 9809458 A	05-03-1998
			SE 9900589 A	07-05-1999
WO 0049827	A	24-08-2000	AU 2954300 A	04-09-2000

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW

(72)発明者 サルヴェラ ユハ
フィンランド エフイーエン-02150 エ
スプー オタカリオ 1セ28

Fターム(参考) 5K033 AA08 CB14 DA19
5K067 AA30 BB04 DD11 DD17 DD36
EE02 EE10 EE24 HH01 JJ71
JJ78

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.